A New Chaos-based Communication Scheme Using Observers

K. Busawon, Rupak Kharel and Z. Ghassemlooy
Northumbria Communication Research Laboratory,
School of CEIS, Northumbria University, Ellison Building,
Newcastle-Upon-Tyne, NE1 8ST, U.K.
krishna.busawon@unn.ac.uk

***Abstract*— In this paper, we propose a new chaos-based communication scheme using observers. The novelty lies in the masking procedure that is employed to hide the confidential information using the chaotic oscillator. We use a combination of the so-called addition and inclusion methods to mask the information. We compare two observers, the proportional observer (P-observer) and the proportional integral observer (PI-observer) that are employed as receivers for the proposed communication scheme. We show that the P-observer is not suitable for the proposed communication scheme since it imposes unpractical constraints on the messages to be sent. On the other hand, we show that the PI-observer is the best solution for the proposed communication scheme since it allows greater flexibility in choosing the gains of the observer and it does not impose any unpractical restiction on the message.**

I. Introduction

There has been a lot of interest in the problem of synchronisation of chaotic systems for secure communication purposes over the last decade. Indeed, several chaotic communication schemes have been developed using different masking techniques such as the method via addition, chaotic shift keying, chaotic modulation or inclusion etc. [1-10]. The classical masking technique where the message is added to the output of the chaotic oscillator or transmitter as illustrated in Fig. 1.

This method of masking is sometimes known as the chaotic masking [1] in the literature or masking by addition or simply the addition method. In this scheme the chaotic oscillator or transmitter generates a chaotic signal $y(t)$ upon which a message $m(t)$ is superimposed by addition. At the receiver end, the transmitted signal $y_t(t) = y(t) + m(t)$ is processed by an observer in order to produce an estimate $\hat{y}(t)$ of $y(t)$. This implies that a certain degree of robustness must be exhibited by the observer in generating the estimated output $\hat{y}(t)$ - since it is excited by the transmitted signal $y_t(t)$ which obviously provide only partial information about the carrier signal $y(t)$. This also implies that the message should not be of a too high amplitude compared to that of the output. In fact, the message should be at least 20 to 30dB lower than the output of the oscillator [1]. As a result one drawback of this method is that it is difficult to retrieve the message if the power of channel noise is of the order of the power of the message. It is also important to note that the strange attractor of the oscillator is not modified by the message. The original message $m(t)$ is generally recovered via a message recovery module which performs some sort of inversion. In this particular case, the message is recovered or retrieved by performing the following substraction:

$$y_t(t) - \hat{y}(t) = y(t) - \hat{y}(t) + m(t). \qquad (1)$$

The observer is generally designed such that $\lim_{t\to+\infty} |y(t) - \hat{y}(t)| \to 0$. As a result, the difference $\xi(t) = y_t(t) - \hat{y}(t) = m_r(t)$ will asymptotically converge to the transmitted message $m(t)$. Obviously, if $\hat{y}(t)$ converges exponentially to $y(t)$, then we will have a better convergence between $m_r(t)$ and $m(t)$. However, it has been shown that the above scheme is not perfectly secure [2]. In effect, it has been shown that this method of masking is sensitive to external attack.

One alternative scheme to overcome this problem is to employ the so-called method of inclusion [3-4] as shown in Fig. 2. In this method the message is either included in a state or the derivative of the state or in the parameter of the system. This method has been proven to be more secure than the chaotic masking by addition since it uses the message to modify the strange attractor of the chaotic oscillator. However, care should be taken so that the inclusion of the message does not disturb the chaotic regime of the oscillator and bring it to a normal periodic motion. On the other hand, with the inclusion method the message recovery becomes more difficult since it requires some sort of inverse system at the receiver end [5-6]. To handle the above two issues, we propose to employ, in this work, a combination of the above two masking techniques

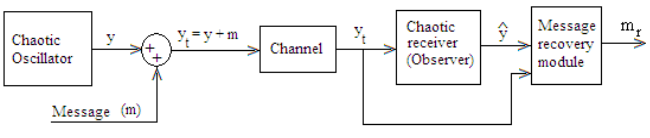

Fig. 1. Chaotic masking

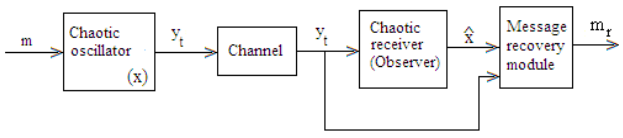

Fig. 2. Inclusion method

978-1-4244-1876-3/08/$25.00 ©2008 IEEE

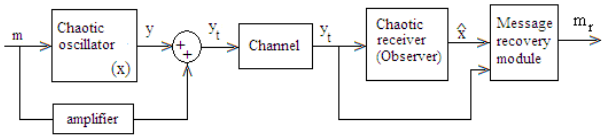

Fig. 3. Combination of inclusion and chaotic masking method

as illustrated in Fig. 3.

In effect, we propose to inject the message in the oscillator as well as adding the message to the output of the oscillator. We test this new chaotic communication scheme by using the Duffing oscillator as the transmitter. We next study the effect of employing two different observers as the receiver system; namely a proportional observer (P-observer) and a proportional integral observer (PI-observer) [7]. We show that the proportional observer does not work properly for this particular oscillator. In effect, a residual term is always present in the error dynamics of the observer which implies that the convergence of the observer is only asypmtotic. Also, the inclusion of the message changes the chaotic regime of the oscillator into a normal periodic behaviour.

On the other hand we show that the PI-observer is the most adequate solution for this scheme using the Duffing oscillator. The gain of the PI-observer can be chosen in such a way that the effect of the message is negligible in the error dynamics. Simulations are carried out to support the above argument and to show the performance of both observers. Finally, some concluding remarks are made.

II. Application using the Duffing oscillator

In this section, we shall compare the above P and PI-observer-based synchronization scheme described in Fig. 3 by using the Duffing oscillator as the drive system.

Consider the Duffing oscillator which is described by the following equations [8]:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = -\dfrac{x_1}{4} - x_1^3 + 11\cos t \end{cases} \tag{2}$$

We assume that the state variable x_1 is measured, i.e. the output equation is $y = x_1$ so that the system can be written in matrix form as:

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}f(y) + \mathbf{h}(t) \\ y = \mathbf{C}\mathbf{x} \end{cases} \tag{3}$$

where

$$\begin{aligned} \mathbf{A} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ \mathbf{B} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \mathbf{C} &= \begin{pmatrix} 1 & 0 \end{pmatrix}, \ f(y) = -\frac{y}{4} - y^3 \\ \mathbf{h}(t) &= \begin{pmatrix} 0 \\ 11\cos t \end{pmatrix}. \end{aligned}$$

Here the masked system is given by:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = -\dfrac{y_t}{4} - y_t^3 + 11\cos t + m \\ y_t = x_1 + d_0 m \end{cases} \tag{4}$$

whereby it can be observed that the message is included on the derivative of the second state variable x_2 and is also added to the output of the system. The masked system can be written in matrix form as:

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}f(y_t) + \mathbf{h}(t) + \mathbf{B}m \\ y_t = \mathbf{C}\mathbf{x} + d_0 m \end{cases} \tag{5}$$

We shall assume that the channel is ideal throughout this work.

A. P-observer-based scheme

A classical Luenberger type observer for the masked system (5) is given by:

$$\dot{\hat{\mathbf{x}}} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{B}f(y_t) + \mathbf{h}(t) + \mathbf{K}(y_t - \mathbf{C}\hat{\mathbf{x}}) \tag{6}$$

where the gain $\mathbf{K} = \begin{pmatrix} k_1 & k_2 \end{pmatrix}^T$ is chosen such that the matrix $(\mathbf{A} - \mathbf{K}\mathbf{C})$ is stable.

More precisely, we have

$$\begin{cases} \dot{\hat{x}}_1 = \hat{x}_2 + k_1(y_t - \hat{x}_1) \\ \dot{\hat{x}}_2 = -\dfrac{y_t}{4} - y_t^3 + 11\cos t + k_2(y_t - \hat{x}_1) \end{cases} \tag{7}$$

or

$$\begin{cases} \dot{\hat{x}}_1 = \hat{x}_2 + k_1(x_1 + d_0 m - \hat{x}_1) \\ \dot{\hat{x}}_2 = -\dfrac{y_t}{4} - y_t^3 + 11\cos t + k_2(x_1 + d_0 m - \hat{x}_1) \end{cases} \tag{8}$$

By setting $\mathbf{e} = \mathbf{x} - \hat{\mathbf{x}}$, we can determine the error dynamics which is given by:

$$\begin{cases} \dot{e}_1 = e_2 - k_1 e_1 + k_1 d_0 m \\ \dot{e}_2 = -k_2 e_1 + m + k_2 d_0 m \end{cases} \tag{9}$$

or

$$\begin{pmatrix} \dot{e}_1 \\ \dot{e}_2 \end{pmatrix} = \begin{pmatrix} -k_1 & 1 \\ -k_2 & 0 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} + \begin{pmatrix} k_1 d_0 \\ 1 + k_2 d_0 \end{pmatrix} m \tag{10}$$

We wish to make the above equation independent of m. For this we choose $d_0 = -k_2^{-1}$. Finally, we obtain

$$\begin{aligned} \begin{pmatrix} \dot{e}_1 \\ \dot{e}_2 \end{pmatrix} &= \begin{pmatrix} -k_1 & 1 \\ -k_2 & 0 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} + \begin{pmatrix} k_1 d_0 \\ 0 \end{pmatrix} m \\ &= (\mathbf{A} - \mathbf{K}_p\mathbf{C})\,\mathbf{e} + \mathbf{E}m \end{aligned} \tag{11}$$

Unfortunately, one cannot choose $k_1 = 0$ otherwise the eigenvalues of $(\mathbf{A} - \mathbf{K}_p\mathbf{C})$ would lie on the imaginary axis and the error dynamics would be only marginally stable. On the other hand care should be taken not to choose k_1 too small otherwise the stability of the matrix $(\mathbf{A} - \mathbf{K}_p\mathbf{C})$ will be compromise. There should be therefore a trade-off in the choice of k_1.

Finally, when the convergence is achieved, the message is retrieved by performing the following difference

$$y_t(t) - \hat{y}(t) = y(t) - \hat{y}(t) + d_0 m(t) = \xi(t).$$

Since $\lim_{t \to +\infty} |y(t) - \hat{y}(t)| \to 0$, we have

$$m(t) \approx \frac{\xi(t)}{d_0} = m_r(t). \tag{12}$$

1) Simulation results: A simulation of the above observer and message recovery method was carried out. The poles of the observer were set as $p_1 = -0.1 = p_2$ so that $k_1 = 0.2$ and $k_2 = 0.01$. Therefore, $d_0 = -k_2^{-1} = -100$. In addition, we have used the following numerical values: $x_1(0) = x_2(0) = 0$, $\hat{x}_1(0) = 0$ and $\hat{x}_2(0) = 0.1$. The message consisted of a set of a sinusoidal message of amplitude of 1 and a frequency of 1 rad/s; that is $m(t) = \sin t$. Fig. 4 and Fig. 5 show the profile of the state variables $x_1(t)$ and y_t respectively. We can readily see that with the inclusion of the message into the oscillator, the chaotic regime no longer exists. The oscillator is operating into a normal periodic mode. Fig. 6 depicts the original message and the recovered message (in dotted lines). We can observe a delay in the recovered message due to the presence of the term $\mathbf{E}m$ in the error dynamics (11).

In order to get back the chaotic behaviour of the oscillator, the amplitude of the message had to be reduced significantly; more than 100 times! In fact, even though not shown here, it is only when $m(t) = 0.01 \sin t$ that the chaotic regime appeared again. Consequently, the above communication scheme cannot work properly in practice if a proportional observer is employed as a receiver. In the next section we show that a PI-observer is the suitable observer for the proposed communication scheme.

B. PI-observer-based scheme

In this case, an integrator is place at the receiver end of the communication system as shown in Fig. 7.

The transmitted message and its integral are both fed to the observer in order to provide an estimate of the state of the oscillator. To design the PI-observer, we set $x_0 = \int_0^t y_t(\tau)\, d\tau = y_I$. In other words $\dot{x}_0 = y_t = x_1 + d_0 m$. We then have the following augmented system:

$$\begin{cases} \dot{x}_0 = x_1 + d_0 m \\ \dot{x}_1 = x_2 \\ \dot{x}_2 = -\dfrac{y_t}{4} - y_t^3 + 11\cos t + m \\ y_t = x_1 + d_0 m \\ y_I = x_0 \end{cases} \tag{13}$$

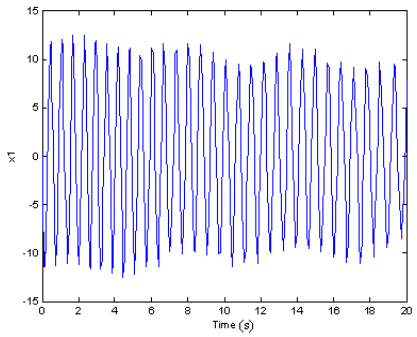

Fig. 4. x_1 with P-observer

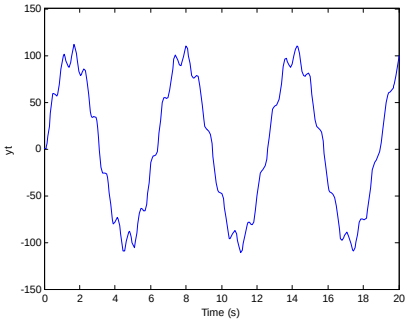

Fig. 5. y_t with P-observer

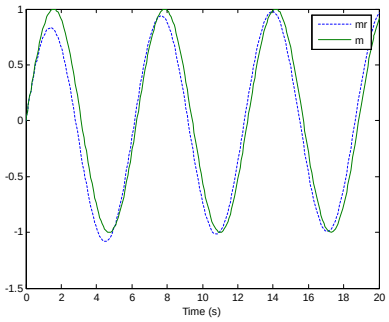

Fig. 6. Message recovery with P-observer

The PI-observer for the above system is given by:

$$\begin{cases} \dot{\hat{x}}_0 = \hat{x}_1 + k_0(x_0 - \hat{x}_0) + l_0(y_t - \hat{x}_1) \\ \dot{\hat{x}}_1 = \hat{x}_2 + k_1(x_0 - \hat{x}_0) + l_1(y_t - \hat{x}_1) \\ \dot{\hat{x}}_2 = -\dfrac{y_t}{4} - y_t^3 + 11\cos t + k_2(x_0 - \hat{x}_0) + l_2(y_t - \hat{x}_1) \end{cases} \tag{14}$$

where $\mathbf{K}_p = \begin{pmatrix} k_0 & k_1 & k_2 \end{pmatrix}^T$ is the proportional gain and $\mathbf{L}_I = \begin{pmatrix} l_0 & l_1 & l_2 \end{pmatrix}^T$ is the integral gain.

By setting $e_i = x_i - \hat{x}_i$; $i = 0..2$, one can easily check that the error dynamics is given by:

$$\begin{cases} \dot{e}_0 = e_1 - k_0 e_0 - l_0(e_1 + d_0 m) + d_0 m \\ \dot{e}_1 = e_2 - k_1 e_0 - l_1(e_1 + d_0 m) \\ \dot{e}_2 = -k_2 e_0 - l_2(e_1 + d_0 m) + m \end{cases} \tag{15}$$

After some simplification we obtain:

$$\begin{cases} \dot{e}_0 = -k_0 e_0 + (1 - l_0)\, e_1 + (1 - l_0)\, d_0 m \\ \dot{e}_1 = -k_1 e_0 - l_1 e_1 + e_2 - l_1 d_0 m \\ \dot{e}_2 = -k_2 e_0 - l_2 e_1 + (1 - l_2 d_0)\, m \end{cases} \tag{16}$$

We choose the integral gain $\mathbf{L}_I = \begin{pmatrix} l_0 & l_1 & l_2 \end{pmatrix}^T$ such that:

$$\begin{aligned} l_1 &= 0 \\ 1 - l_0 &= \epsilon \\ -l_2 d_0 + 1 &= 0 \end{aligned}$$

We therefore obtain:

$$\begin{cases} \dot{e}_0 = -k_0 e_0 + \epsilon e_1 + \epsilon d_0 m \\ \dot{e}_1 = -k_1 e_0 + e_2 \\ \dot{e}_2 = -k_2 e_0 - l_2 e_1 \end{cases} \tag{17}$$

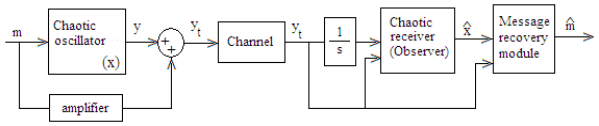

Fig. 7. PI-observer based scheme

The above error dynamics can be written in matrix form as:

$$\begin{pmatrix} \dot{e}_0 \\ \dot{e}_1 \\ \dot{e}_2 \end{pmatrix} = \begin{pmatrix} -k_0 & \epsilon & 0 \\ -k_1 & 0 & 1 \\ -k_2 & -l_2 & 0 \end{pmatrix} \begin{pmatrix} e_0 \\ e_1 \\ e_2 \end{pmatrix} + \begin{pmatrix} \epsilon d_0 \\ 0 \\ 0 \end{pmatrix} m$$
$$= \mathbf{F}\mathbf{e} + \bar{\mathbf{E}}m \qquad (18)$$

Comparing this equation with (11) we can choose d_0 independently of the proportional gain $\mathbf{K}_p$. In addition, one can choose d_0 as small as possible in order to eliminate the effect of the message on the error dynamics. Finally, the proportional gain $\mathbf{K}_p$ is chosen such that the matrix $\mathbf{F}$ is stable.

1) Simulations results:: For simulation purposes we have chosen $d_0 = \epsilon = 0.1$ so that $l_0 = 0.9$ and $l_2 = 10$. In addition, $x_0(0) = x_1(0) = x_2(0) = 0$, $\hat{x}_0(0) = \hat{x}_1(0) = 0$ and $\hat{x}_2(0) = 0.1$. The poles of the observer are all set at $p = 0.1$ so that $k_0 = 0.3$, $k_1 = -99.7$, $k_2 = -29.99$. As before, the message consisted of a set of a sinusoidal message of amplitude of 1 and a frequency of 1 rad/s; that is $m(t) = \sin t$. Fig. 8 and Fig. 9 show the profile of the state variable x_1 and the transmitted message y_t. Here we can see that the chaotic regime is maintained and the transmitted message is scrambled and not discernible. Fig. 10 shows the performance of the observer in accurately estimating the message with very little delay. It is important to note it is because the PI-observer allows to choose the proportional and integral gains fairly independently that this particular scheme works better that with the proportional observer. In effect, with the proportional observer, the gain has to deal with the stability of the error dynamics as well as to reduce the effect of the message on the error dynamics. Hence there is too much constraints imposed of the sole proportional gain. On the other hand, with the PI-observer the integral gain is used to deal the stability of the error dynamics while the proportional gain is used to reduce the effect of the message on the error dynamics.

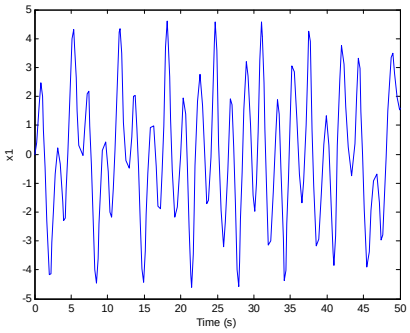

Fig 8. x_1 with PI-observer

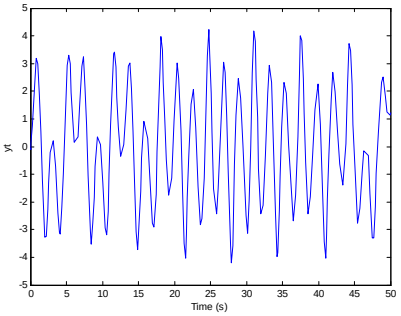

Fig. 9. y_t with P-observer

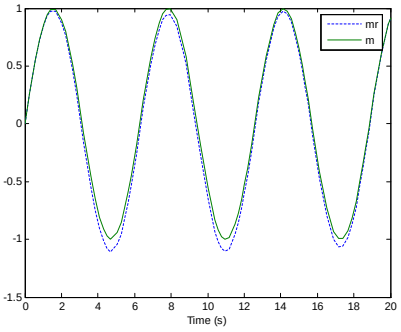

Fig. 10. Message recovery using PI-observer

III. Conclusions

In this paper we have proposed a new chaos-based communication scheme using observers. The main novelty lies in the masking method employed. It uses a combination of the addition and inclusion method into to mask the message. This was done mainly to facilitate the recovery of the message. We have compared two observers that are employed as receivers for the proposed communication scheme namely: the proportional observer (P-observer) and the proportional integral observer (PI-observer). We have shown that the P-observer is not suitable for the proposed communication scheme since it imposes unpractical constraints on the messages to be sent if the communication has to be kept secure. On the other hand, we show that the PI-observer is the best solution for the proposed communication scheme since it allows greater flexibility in choosing the gains of the observer and it does not impose any unpractical restriction on the message. This is mainly due to the fact that, with the PI-observer, the integral gain is used to deal the stability of the error dynamics while the proportional gain is used to reduce the effect of the message on the error dynamics. Finally, it is important to note that we have assumed that the channel is perfect throughout this work. However, in practical situations, the model of the channel and the noise has to be taken into account as well as the time delay involved in the message transmission. Consequently, an important

topic of research, which is currently under investigation, is to take all these considerations into account in the design of the proposed communication scheme.

REFERENCES

[1] Cuomo, K. M. and Oppenheim, A. V., "Circuit implementation of synchronized chaos with applications to communications", *Phys. Rev. Lett.* Vol. **71**, 65-68, 1993.

[2] K. M. Short, "Steps towards unmasking secure communications", *Int. J. Bifurcation and Chaos*, Vol. **4**, pp. 959-977, 1994

[3] Barbot, J.P. Belmouhoub and Boutat-Badas, L., "Observability bifircations: applications to cryptography", *Chaos in Automatic control*, Taylor and Francis, 2005.

[4] Yang, T. and Chua, L.O., "Secure communication via chaotic parameter modulation", *IEEE Transactions on Circuits and Systems: I* Vol. **44**, pp. 469-472, 1997.

[5] Boheme, F., and Bauer, A., "Information transmission by chaotizing", *Proc. NDES'94*, Krakow, pp. 163-168, 1994.

[6] Feldmann, U., Hasler, M., and Shwartz, W., "Communication by chaotic signals: the inverse system approach", *Proc. ISAS'95*, Seattle, pp. 680-683, 1995.

[7] Busawon, K. and Kabore P., "Disturbance attenuation using proportional integral observers", *Int. J. Control,* Vol. **74**, No.6, 618-627, 2001.

[8] P. Johnson and K. Busawon, "Chaotic synchronization using PI-observers", *Proc. 1st Conference in Chaos and communication, CHAOS06*, Reims, France, 2006.

[9] Kolumban, G, Kennedy, MP, Chua, LO. "The role of synchronization in digital communications using chaos .1. Fundamentals of digital communications." *IEEE Trans. Circuits Syst. I-Fundam. Theor. Appl.* Vol. 44: 927, 1997.

[10] Morgul, O., Solak, E. and Akgul, M., "Observer based chaotic message transmission," *Int. J. Bifurcation and Chaos*, Vol. **13**, No.4, 1003-1017, 2003.